# ELECTRONIC WARFARE


**AIR FORCE DOCTRINE DOCUMENT 2-5.1**

**XX OCTOBER 1998**

# FOREWORD

**Aerospace power and technology have always been tightly bound together throughout the history of air and space operations.** This linkage is very evident in the combat machines, devices, and tactics needed to survive in the aerospace environment. The use of radio and radar early in World War II as the means to find targets on the surface and in the air illustrates the first exploitation of the electromagnetic spectrum in aerial warfare. The advent of countermeasures to these systems produced what we now consider electronic warfare. Today's weapon systems and support systems rely on radio, radar, infrared, electro-optical, ultraviolet, and/or laser technologies to function in peace and war. Unhampered use of the electromagnetic medium is vital to assure the success of any modern military operation. Coalition forces in OPERATION DESERT STORM operated "at will" over Iraq and Kuwait after gaining control of the electromagnetic spectrum early in the war. Air Force Doctrine Document 2-5.1, *Electronic Warfare*, is written to provide a basis for understanding, planning, and executing this portion of aerospace warfare.

RONALD E. KEYS

Major General, USAF

OPR: HQ AFDC/DR (Maj Raymond L. Laffoon, Jr.)
Certified by: AFDC/DR (Lt Col Thomas A. Bowermeister, USAF)
Pages:
Distribution: F, J
Approved by: Ronald E. Keys, Maj Gen, USAF
Commander

1

# TABLE OF CONTENTS

# INTRODUCTION

## PURPOSE

This document establishes operational doctrine for United States Air Force electronic warfare operations. It articulates fundamental Air Force principles for the application of combat force and provides commanders operational level guidance on the employment and integration of Air Force resources to achieve desired objectives. Air Force Doctrine Document (AFDD) 2-5.1 supports operations espoused in joint doctrine.

## APPLICATION

AFDD 2-5.1 applies to all active duty Air Force agencies that may be involved in planning or conducting electronic warfare operations, including the United States Air Force Reserve (USAFR), Air National Guard (ANG), and civilian Air Force personnel. The doctrine in this document is authoritative but not directive. Therefore, commanders need to consider not only the contents of this AFDD, but also the particular situation in which they find themselves—national military objectives, forces available, enemy capabilities, rules of engagement—when accomplishing their assigned missions.

## SCOPE

This doctrine provides guidance for planning and conducting Electronic Warfare operations in support of national and joint force commander (JFC) campaign objectives.

# CHAPTER ONE

# BACKGROUND

> *No enterprise is more likely to succeed than one concealed from the enemy until it is ripe for execution.*
>
> Niccolo Machiavelli, *The Prince*, 1521

Modern military forces rely heavily on a variety of complex, high technology, electronic offensive and defensive capabilities. Today's weapons and support systems employ radio, radar, infrared, optical, ultraviolet, electro-optical, or laser technology. Commanders must prepare to operate weapons systems in an intensive and nonpermissive electromagnetic environment aggravated by both intentional and unintentional emissions from friendly, neutral, and enemy forces. Success requires awareness, dynamic planning, and flexibility at all times and at all levels of war to effectively accomplish the mission's objectives and tasks. **Clear access to selected portions of the electromagnetic spectrum is critical for weapon system effectiveness.**

**EW is any military action involving the use of electromagnetic and directed energy to manipulate the electromagnetic spectrum or to attack an adversary.** This is not limited to radio or radar frequencies but includes infrared and optical regions. EW assists aerospace forces to gain access and operate without prohibitive interference from adversary systems. During Operation DESERT STORM, effective force packaging, which included self-protection, standoff, and escort jamming and antiradiation attacks, contributed to the Air Force's extremely low loss rate.

**The three major subdivisions of EW are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).** *All three contribute to air and space operations, including the integrated Information Operations (IO) effort.* Control of the electromagnetic spectrum is gained by protecting friendly systems and countering adversary systems. EA limits adversary use of the electronic spectrum; EP enhances the use of the electronic spectrum for friendly forces; and ES enables the commander's accurate estimate of the situation in the operational area**.** EA and ES must be carefully integrated with EP in order to be effective. The responsible commander must ensure maximum coordination and deconfliction between EW, Intelligence, Surveillance and Reconnaissance (ISR), and other communication activities.

Control of the electromagnetic spectrum can have a major impact on the success of military operations across the different levels of conflict. Proper employment of EW enhances the ability of US operational commanders to achieve objectives. **EW is a force multiplier**. *When EW actions are integrated with military operations, a synergistic effect is achieved, attrition is minimized, and effectiveness is enhanced*.

**EW IN VIETNAM**

"Countermeasures helped keep American aircraft losses to a manageable rate. One Air Force officer estimated that ECM reduced losses by 25 percent, while a Navy officer put the figure at 80 percent. Nevertheless, air operations were expensive both in losses and effort. Communist gunners proved a worthy and resourceful foe, although limited by second-rate Soviet equipment. Yet, despite the able Communist air defense tactic and their adaptation to the changing tactical situation, the American airmen gradually increased their edge. The big improvement for the offensive side came with the use of ECM and antiradiation and standoff weapons. These increased accuracy and decreased losses. In the full-scale operations of Linebacker II, the American airmen showed that massive application of modern aircraft with modern equipment could succeed against defenses limited in numbers and quality."

**Kenneth P. Werrell**
**Archie, Flak, AAA, and SAM: A Short Operational History of Ground-Based Air Defense**

**Air Force EW strategy embodies the art and science of employing military assets to improve operations through control of the electromagnetic spectrum.** EW exploits weaknesses in an adversary's ability to operate and apply force against its offensive, defensive, and supporting capabilities across the electromagnetic spectrum. An effective EW strategy requires an integrated mix of disruptive and destructive systems to reduce force attrition, and to protect our weapons systems, components, and communications-electronics systems from the threat. Although operational commands differ in the use of electronic warfare, EW strategy has elements common to all.

**Electronic warfare is intimately tied to advances in technology.** The advent of radar early in World War II started the "move – countermove" developments of radar, sensors, jammers, and countermeasures. Radar first proved its effectiveness early in World War II. Shortly after the development of radar, chaff (then called Window) was developed as an effective countermeasure. Concurrently, airborne jammers were developed to minimize the effectiveness of radar. The advent of the Cold War witnessed the development of radar with effective Electronic Counter Countermeasures (ECCM) (now called Electronic Protection), along

with the jammers and countermeasures to counter ECCM. Conflicts in Vietnam and the Middle East were deadly reminders of ineffective EW against advanced threats and the intense effort required to effectively counter these threats. Today's technology includes threats operating with the use of microwave technology, lasers, electro-optics, portable systems, and computers with the associated automation and connectivity. EW is not limited to radio or radar frequencies but includes optical and infrared regions, as well as those in which directed energy (DE) weapons might function. *Anticipating tomorrow's technology is vital to the success of EW and the survivability of friendly forces.*

**Control of the electromagnetic spectrum is an essential and critical objective in the success of today's military operations and is applicable at all levels of conflict.** EW considerations must be fully integrated into operational plans in order to be effective. Commanders must be prepared to operate in a nonpermissive electromagnetic environment and understand EW's potential to increase force effectiveness.

# CHAPTER TWO

# EW OPERATIONAL CONCEPTS

> ***O divine art of subtlety and secrecy!***
> *Through you we learn to be invisible, through you inaudible; and hence hold the enemy's fate in our hands.*
>
> **Sun Tzu, *The Art of War*, c. 500bc**

## GENERAL

Military forces depend on the electronic spectrum for many applications including, but not limited to, communications, detection, identification, and targeting. The effective application of electronic warfare in support of mission objectives is critical in our ability to find, fix, track and target ($F_2T_2$), while preventing our adversaries the same capability. Electronic Warfare uses the tenets of Control, Exploit, and Enhance to be effective. The three tenets are employed by the three components of EW: Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES). Proper application of the components produces the effects of detection, denial, disruption, deception, and destruction in varying degrees to enhance overall mission objectives.

## EW TENETS

**Control.** *To control is to dominate the electromagnetic spectrum, directly or indirectly, so that friendly forces may attack the adversary and protect themselves from attack.* Electronic warfare

has offensive and defensive aspects that work in a "move-countermove" fashion. Often, these aspects are used simultaneously and synergistically to support the mission. For example, the offensive denial of a command and control network by jamming disrupts the adversary's ability to marshal forces that would otherwise engage a friendly strike force.

**Exploit.** *To exploit is to use the electromagnetic spectrum to the advantage of friendly forces.* Friendly forces can use detection, denial, disruption, deception, and destruction in varying degrees to impede the adversary's decision loop. One can envision electronic warfare as attacks against the sensors or the "eyes and ears" of the adversary.

**Enhance.** *To enhance is to use EW as a force multiplier. Control and exploitation of the electromagnetic spectrum improves the likelihood of mission success.* During the first night of Operation DELIBERATE FORCE, jammers negated adversary SAM systems, allowing NATO aircraft unimpeded access to prime command and control targets in Bosnia.

## ELECTRONIC WARFARE COMPONENTS

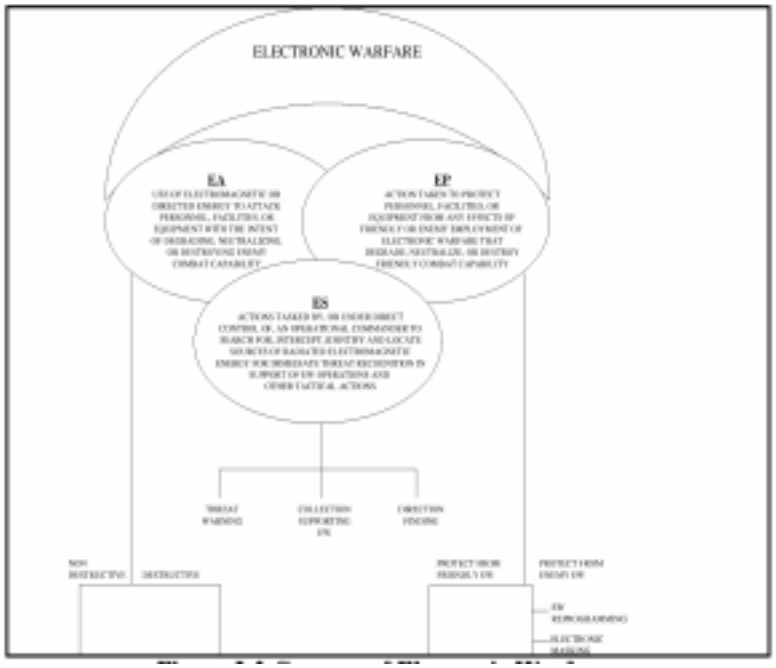



**Figure 2-1, Concept of Electronic Warfare**

The three major components of Electronic Warfare are Electronic Attack (EA), Electronic Protect (EP), and EW Support (ES).

**Electronic Attack (EA). EA is the division of EW involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.** EA is used to prevent or reduce an enemy's use of the electromagnetic spectrum. It can be accomplished through denial, disruption, deception and/or destruction, and relies heavily on detection. EA includes active applications such as noise jamming, deceptive jamming,

expendable miniature jamming decoys, and employs electromagnetic or directed energy weapons (HARMs, lasers, radio frequency weapons, particle beams, etc). Chaff and flares, electronic emission control (EMCON), and low observable technologies are passive applications of EA.

**Early EW, Russo-Japanese War, 1904**

"On 8 March 1904, the Japanese attempted to carry out an attack on Russian ships anchored in the inner roads of Port Arthur, and thus not visible to the open sea. They sent two armoured cruisers, *Kasuga* and *Nisshin*, to bombard the roads by indirect fire, using a small destroyer favourably located nearer the coast to observe where the shells fell and to transmit correct firing instructions to the cruisers. However, a wireless operator at the Russian base heard the signals the Japanese ships were exchanging and, although he did not really understand what he was doing, he instinctively pressed the signalling key of his spark transmitter in the hope that this might interfere in some way with the communications between the enemy ships. As a result of his instinctive action, no Russian ships were damaged by Japanese naval bombardment that day since the Japanese, their communications jammed, cut short their action and withdrew."

Mario de Arcangelis
Electronic Warfare: From Tsushima to the Falklands and Lebanon Conflicts

Electronic jamming and the suppression of enemy air defenses (SEAD) are elements of EA:

- **Electronic Jamming**. *Electronic jamming causes temporary interruption of electromagnetic systems or equipment.* Early Air Force EW efforts were primarily directed toward electronically jamming hostile radars to hide the number and location of friendly aircraft and to degrade the accuracy of radar controlled weapons. Currently, jamming enemy sensor systems limits the information on force movements, causes confusion, and masks friendly movements. When applied against command and control systems, jamming slows the enemy's decision-making process, causes the enemy to make incorrect decisions, and interferes with the enemy's ability to implement decisions in a timely manner. An adversary

heavily dependent on centralized control and execution for force employment is highly susceptible to jamming.

- **Suppression of Enemy Air Defenses (SEAD).** *SEAD is that activity which neutralizes, destroys, or temporarily degrades surface-based enemy air defenses by destructive and/or disruptive means*. The goal of SEAD operations is to provide a favorable situation in which friendly tactical forces can perform their missions effectively without interference from electronically directed enemy air defenses. SEAD is integral to the counterair mission and directly contributes to obtaining air superiority. This may involve using electromagnetic radiation or the destruction of elements of an enemy's integrated air defense system (IADS). During hostilities, enemy air defensive systems will probably challenge friendly air operations. Aircraft tasked to perform SEAD may be employed to locate and degrade, neutralize, or destroy airborne and ground-based emitters. Normal SEAD targets are early warning, acquisition (ACQ), ground-controlled intercept (GCI), surface-to-air missile (SAM), and antiaircraft artillery (AAA) radars; and air intercept (AI) radars. SEAD is effective against communications jammers; air defense jammers, and communication transmitters. All Air Force functions can be enhanced with the employment of SEAD operations

**Electronic Protection (EP). EP includes the actions taken to protect friendly personnel, facilities, and equipment from**

**Early EW, First World War, 1916**

"No one is quite sure when EW began. We do know that as far back as 31 may 1916, the Admiral of the Fleet, Sir Henry Jackson, employed EW as a preliminary to the battle of Jutland. Sir Henry used evidence of coastal radio direction finders under admiralty supervision to detect movement of the German fleet. The changes in the apparent directions of arrival of radio signals from the enemy fleet were very slight, but Sir Henry dared to move the opposing British fleet on the basis of this information."

**AFP 51-45**
**15 September 1987**

**any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability.** Proper integration of electronic counter countermeasures and various security measures can prevent effective enemy application of disruption, destruction, deception, or denial. Reliance on instant communication and precision navigation demands EP safeguards. Proper frequency management is a key element in preventing adverse effects (i.e. jamming friendly forces) by friendly forces.

**EW Support (ES). ES is that division of electronic warfare involving actions tasked by, or under the direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition.** Commanders, aircrews, and operators use ES to provide near real-time information to supplement information from other intelligence sources. Additionally, ES information can be correlated with other intelligence information to provide a more accurate picture of the battlespace. This information can be developed into an Electronic Order of Battle (EOB) for situational awareness and may be used to develop new countermeasures. ES data can be used to produce signal intelligence (SIGINT) which includes communications intelligence (COMINT) and electronic intelligence (ELINT). Thus, ES provides information required to effectively deny the enemy's use of the electromagnetic spectrum while ensuring friendly use. It allows for immediate decisions involving electronic warfare operations and other tactical actions such

as threat avoidance, targeting and homing. The passive nature of ES allows it to be effectively employed during peacetime.

## EW EFFECTS

**EW is waged throughout the electromagnetic spectrum to secure and maintain effective control and use of the spectrum by friendly forces and inhibits use by the enemy through effective integration of detection, denial, deception, disruption, and damage/destruction.** This control is not limited to radio or radar frequencies but includes optical and infrared regions, as well as those in which directed energy (DE) weapons might function. The operational application of EW is not limited to manned airborne application. It is also applied from land and space by manned and unmanned vehicles. Various applications of detection, denial, deception, disruption, and damage/destruction result in the proper employment of EW.

**Detection.** ***Detection is*** *assessing the electromagnetic environment to include radar/radio frequency, electro-optics/laser and the infrared spectrums using active and passive means.* It is the first step in EW. Effective mapping of the electromagnetic environment is essential to develop an accurate electronic order of battle (EOB) for effective decision making and to manipulate the electromagnetic spectrum to accomplish mission objectives. These various means include on-board receivers, space based systems, Unmanned Aerial

Vehicles (UAV), Human Intelligence (HUMINT), and ISR. Detection supports EA, EP, and ES. Electronic detection can lead to avoidance of hostile systems, which is often the best course of action. When avoidance is not possible, it becomes necessary to deny, deceive, disrupt, or destroy the enemy's electronic systems.

**Denial.** *Denial is controlling the information an adversary receives and preventing the adversary from gaining accurate information about friendly forces.* For example, effective denial can be accomplished through traditional noise jamming techniques designed to block communications channels or radar scope presentations, or through more advanced electronic deception techniques or destructive measures.

**Deception**. *Deception is designed to confuse or mislead an adversary's decision-maker or operator*. The objective is to exploit the decision-making loop of the opposing commander thus making it difficult to distinguish between reality and the adversary's perception of reality. If an adversary relies on electromagnetic sensors to gather intelligence, deceptive information can be channeled into these collection systems to mislead and cause confusion. Deception efforts must stimulate as many adversary information sources as necessary to achieve the desired objective. Multisensor deception can increase the adversary 's confidence about the "plausibility" of the deception story. Deception efforts are coordinated with the tactical deception officer, and considered during development of an overall deception plan. Operational Security is critical to an effective deception plan.

**ECM and the Invasion of France**

"Window" was also employed during the D-day landings. On D-day minus 2, the coast of Northern France presented a solid radar front-an active threat to invasion operations. Between Ostend and Cherbourg, there was a major German radar station every 10 miles. Actual count from Brest to Calais showed 6 Chimneys and 6 Hoardings for long-range early warning, 38 Freyas for medium range EW and night fighter control, 42 Giant Wurzburgs for night fighter control and coast gun control for use against low flying aircraft, 17 Coastwatchers, and Small Wurzburgs, one per flak battery.

The first task on D-day was to confuse what remained of the German early warning radar (EWR) system which still posed a formidable threat to operations of allied troop carrier and tug aircraft.

On the night preceding D-day, the confusion was accomplished by Mandrel (anti-Freya) jammers carried in eight Sterling aircraft along the south coast, an in four B-17s spaced to give cover as far as the island of Guernsey. Flying at 18,000 feet for 5 hours, these squadrons screened the approach of airborne forces to the French coast.

Meanwhile, British Bomber Command aircraft carried jammers and dropped Window [chaff] and dummy parachutists inland from the Dover-Calais area. Reacting to these countermeasures, German fighter strength spent most of the night circling over the Calais area. As a result, there were no fighter attacks on the 884 transports and 105 gliders of the 9th Troop Carrier Command which landed or dropped some 15,000 troops.

**AFP 51-45**
**15 September 1987**

Electromagnetic deception as it applies to EW is the deliberate radiation, reradiation, alteration, suppression, absorption, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Deception jammers/transmitters can place false targets on the victim radar's scope, or cause the victim radar to assess incorrect target speed, range, or azimuth. Most of them operate by receiving the pulse of energy that strikes the aircraft from the radar, amplifying it, delaying or multiplying it, and re-radiating the altered signal back to the transmitting radar. Types of electromagnetic deception are: (a) manipulative electromagnetic deception, (b) simulative electromagnetic deception, and (c) imitative electromagnetic deception.

Manipulative electromagnetic deception involves action to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may used by hostile forces. An example of this is to mislead the enemy by transmitting a simulated aircraft unique system signature from a non-lethal platform, thereby allowing the enemy sensors to receive and catalog those systems as actual threat aircraft in the area. Low observable technology is a passive form of manipulative electromagnetic deception. By passively manipulating or denying the threat radar from receiving proper return pulses, it alters the perceived size or presence of an aircraft. Electromagnetic deception can use communication or non-communication signals to convey indicators that mislead the enemy. It can also cause the enemy to splinter his intelligence and EW efforts to the point that he loses his effectiveness. Manipulative electromagnetic deception can be used to cause the enemy to misdirect his ES and EA assets and, therefore, cause fewer problems with friendly communications. In this application it is an EP technique.

Simulative electromagnetic deception is action to simulate friendly, notional, or actual capabilities to mislead hostile forces. An example of simulative electromagnetic detection could be the use of chaff to simulate false targets and give the enemy the impression of a larger strike package, or an aircraft jammer transmitting a deceptive technique that misguides a threat's target tracking radar. The radar cannot find the true location of friendly aircraft.

Imitative electromagnetic deception introduces electromagnetic energy into enemy systems that imitate enemy emissions. Any enemy receiver can be the target of imitative electromagnetic deception. This can be used to screen friendly operations. An example is the

use of a repeater jamming technique that imitates enemy radar pulses. These pulses, received by the tracking radar, input incorrect target information into the enemy's system.

Other examples of deception include infrared deception involving manipulation of infrared signatures, radar deception consisting of reradiation of signals through the use of reflectors, transponders, or repeaters, and optical deception by manipulation of the optical region of the electromagnetic spectrum through the use of aerosols, mists, etc. These techniques may be employed individually or in combination with each other. In general, EW deception planning determines how to use electromagnetic means to mislead the adversary and create an advantage for friendly forces.

**Disruption.** *Disruption is degrading or interfering with the enemy's control of its forces in order to limit attacks on friendly forces.* Disruption of the electromagnetic spectrum occurs by using electronic jamming, electronic deception, electronic intrusion, and destruction to enhance successful attacks against hostile forces and to act as a force multiplier.

**Destruction.** *Destruction is the elimination of some or all of an adversary's electronic defenses.* It is the most permanent countermeasure! Target tracking radars and control centers are lucrative targets because their destruction seriously hampers the defense's effectiveness. Destruction requires accurate information on the target's location. A preliminary pre-strike location of a target can be found through the effective application of ES measures. Onboard receivers and direction finding equipment can pinpoint the exact location of the target. Enemy electromagnetic

systems can be destroyed by applying various weapons and techniques, ranging from classical bombing, with conventional munitions, to intense radiation and high energy particle beam overloading. Destruction of certain enemy electromagnetic equipment may be desired as the most effective means of denying the enemy use of the electromagnetic spectrum. The length of suppression gained by destruction depends on the capability and availability of hostile repair and replacement efforts. An example of EW application of destruction would be the use of a High Speed Antiradiation Missile (HARM) against an enemy radar.

## ADDITIONAL FACTORS

**Directed Energy (DE) in EW.** DE is an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. DE is used as a direct means to damage or destroy adversary equipment, facilities, and personnel. *Directed-energy warfare (DEW) is military action involving the use of DE weapons, devices, and countermeasures to either cause direct damage, destruction, and disruption.* It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Possible applications are the laser, radio frequency, and particle beam. DE can be applied to conduct EA, ES, or EP. For example, a laser designed to blind or disrupt optical sensors is, in EW terms, EA. A laser warning receiver designed to detect and analyze a laser signal is, in EW terms, ES. A visor or goggle designed to filter out the harmful wavelength of laser light is, in EW terms, EP.

**Enemy Capabilities.** *Commanders must know their own EW capabilities and those of potential enemies. Mission planning hinges on accurate information.* Each year, new, high technology weapons systems are fielded in increasing numbers. Potential adversaries recognize US dependence on electronically oriented communications and weapons systems. Seeking to take advantage of this fact, some potential adversaries are organized to attack our critical weapons systems control functions and associated communications nodes. Many countries have been purchasing modern and capable weapons systems from a variety of sources. This can result in a complex situation of former friends becoming enemies, or terrorists obtaining certain weapons. Therefore, commanders and staffs must be versed in the employment of hostile and friendly electronic equipment and forces.

**1973 Arab-Israeli War**

The 1973 Arab-Israeli War lasted less than a month, yet it contained all the elements of a much longer war. It was an intense, bitterly contested conflict with each side well equipped with the weapons for modern warfare. The Egyptian and Syrian air defenses at that time were developed from Soviet design. The design stressed overlapping networks of SAM and AAA coverage. This formidable air defense network consisted of the SA-2, SA-3, SA-6, SA-7, the ZSU-23-4, and other AAA systems. While there were proven ECM from the Vietnam War for the SA-2 and SA-3 and infrared (IR) countermeasures, such as flares for the SA-7, the SA-6 proved to be a surprise. The SA-6's radars operated in a portion of the EM spectrum never used before by the Soviets. The Israelis tried to compensate for their lack of ECM against the SA-6 by flying lower, trying to get under its radar coverage. This tactic placed them into the heart of the ZSU-23-4 threat envelope and contributed to the loss of numerous aircraft. This forced the Israelis to adjust their electronic equipment modify their tactics, and seek additional ECM equipment, such as ECM pods and chaff dispensers from the US.

However, before the tactics were changed and the new equipment arrived, the Israelis suffered heavy aircraft losses which taught them a valuable lesson. They learned ECM [EA] is an essential and vital part of the SEAD campaign.

**AFP 51-45**
**15 September 1987**

**Operational Requirements.** Electronic warfare is task oriented. Operational objectives, the tactical situation, the effectiveness and availability of combat systems, and the prevailing domestic and international political climate determine the appropriate application of military

resources. EW planning is not an automatic addition of a specific jamming pod or escort package for a mission. Each task may require a specific EW response in order to attain a desired objective. Commanders and their staffs must consider the threat and assets available to support EW objectives. *The level of EW involvement depends on the specific requirements for accomplishing the objective.*

**Intelligence.** *A thorough knowledge of present enemy capabilities derived from near-real-time intelligence, focused for the operational commander and decision maker on a continuous basis, is essential for any successful military operation.* Knowledge of the enemy's projected military capabilities is required to avoid surprise. Knowing our own capabilities is critical for efficient planning. Accurate intelligence is needed to gauge the intent of an adversary, and this intelligence must be transmitted to the users in a timely manner. There are numerous dedicated reconnaissance systems that can be used to build the various EOBs and electronic data bases required to effectively employ EW. Electronic exploitation for intelligence purposes occurs at all levels of conflict.

**Conclusion.** Electronic warfare through effective use of detection, denial, deception, and destruction provides timely information on the enemy, enhances combat power by disrupting the enemy’s use of the electromagnetic spectrum at critical times, and ensures continued friendly use of the electromagnetic spectrum. The synergistic effects of various EW techniques can significantly disrupt an IADS. Jamming, chaff, and decoys degrade the enemy’s ability to find, fix, track, and target. Radar-guided weapon systems that survive destruction attempts lose some

effectiveness in an EW environment. In short, the probability of successful completion of an assigned mission is greatly increased when EW is properly employed. Electronic warfare in support of operations is a key element in the successful employment of aerospace forces.

# CHAPTER 3
# ELECTRONIC WARFARE ORGANIZATION

> *Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity.*
>
> George Patton

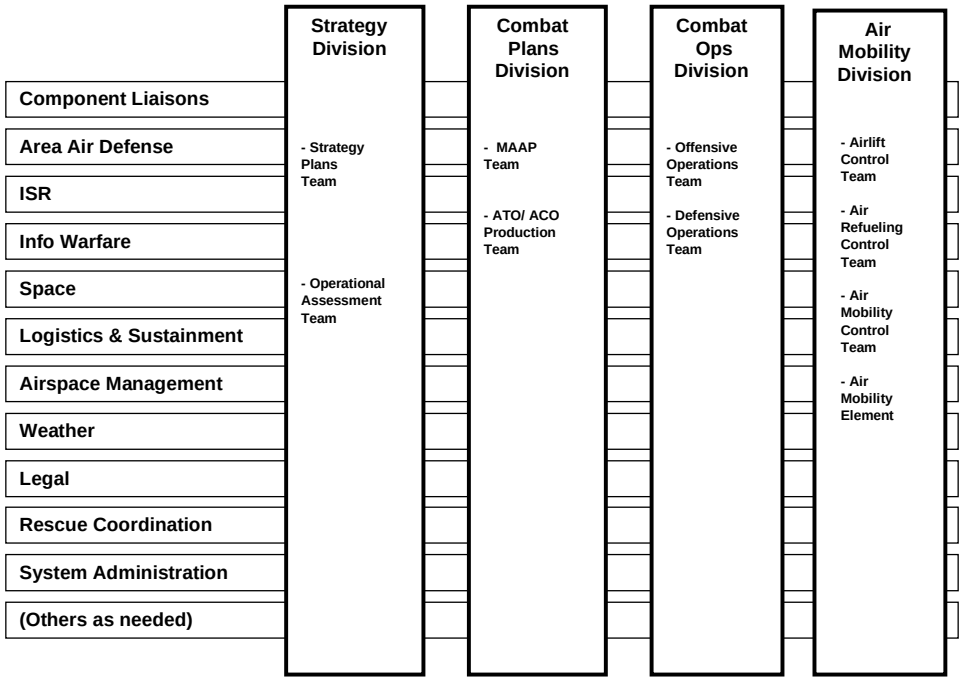
## GENERAL

Electronic warfare assets are organized on the principles of centralized control and decentralized execution. Air Force EW resources are normally employed as part of an Aerospace Expeditionary Task Force (ASETF) and employed at the lowest level providing responsiveness to the Commander, Air Force Forces (COMAFFOR). Appropriate EW expertise must be available at all levels of command where EW coordination, planning, and tasking occur.

**Joint and Combined Operations.** Joint and combined plans must be developed for integrating EW activities. In offensive and defensive applications of EW, close coordination between Services, air traffic control facilities, civil defense activities, and war-related commerce departments is essential. This is required to ensure maximum support, prevent mutual interference, define mutually supporting roles, avoid duplication of effort, provide security, and minimize interference. The importance of integration and coordination cannot be overemphasized, particularly since technological advances are increasing the complexity and interdependence of combat operations. The required deconfliction and coordination of EW support should be accomplished at the Joint Air Operations Center (JAOC). Considerations must include the impact of EW on command and control (C2), information activities, and interrelated requirements for use of the electromagnetic spectrum. Specific guidance on organization and procedures are covered in Joint Pub 3-51, *Joint Doctrine for Electronic Warfare.*

Specialized assets are limited in number; therefore, operational command of these forces should not be delegated lower than the Joint Force Air Component Commander (JFACC). Wing and unit level staffs and individual aircrews develop the detailed tactical planning for specific EW missions. Individual operators must keep current in systems employment and the threat.

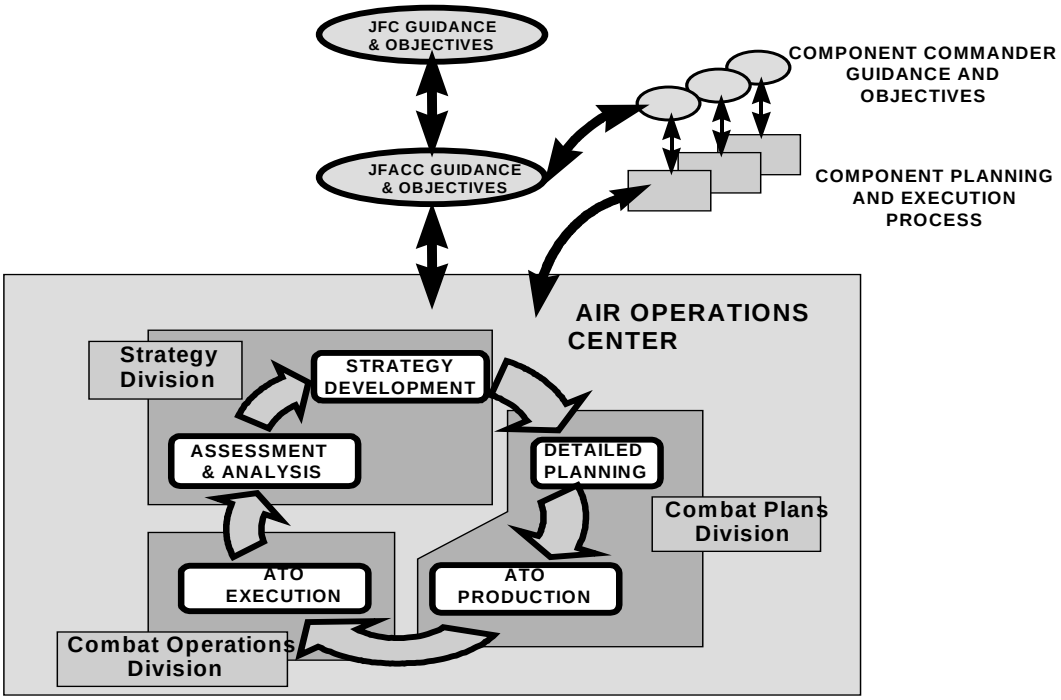
## AOC PLANNING AND EXECUTION PROCESS




**Notional AOC with Representative Core, Specialty, and Support Teams**

This diagram illustrates all four major divisions and several support and specialty teams. The mission will determine the actual mix of divisions and teams in the AOC; not all divisions and teams may be needed. Refer to AFI 13-AOC for more complete discussion of all teams, processes, and supporting systems.

Fundamental to the AOC is an integrated team controlled by the AOC Director. Personnel supporting the EW function typically work through the Information Warfare (IW) cell of the AOC. The IW cell is charged with coordinating the offensive and defensive aspects of IW to include special programs and integration IW efforts with the Joint Aerospace Operations Plan (JASOP). Those individuals should represent all aspects of tactical and strategic EW planning and execution and work closely with the intelligence personnel. This team's expertise ensures that all aspects of EW is fully integrated into strategy development, operational level assessment, detailed planning, ATO production, and execution functions.




The Aerospace Planning and Execution Process

## EW SUPPORT TO THE JOINT FORCE AIR COMPONENT COMMANDER (JFACC)

The JFC will normally designate a JFACC to exploit the capabilities of joint aerospace operations through a cohesive JASOP and a responsive and integrated control system. The JFC must clearly define EW objectives and ensure that assets supporting these objectives are properly employed and integrated throughout military operations. The JAOC formulates plans and coordinates EW activities based on the JFACC's guidance, which is based on JFC objectives. It receives, assembles, analyzes, processes, and disseminates all-source intelligence required for EW planning. EW support assets are tasked through the air tasking order (ATO). EW planners will support the JFACC as follows:

- ✪ Develop a joint EW strategy.
- ✪ Task, plan, coordinate, and allocate the joint EW capabilities/forces made available to the JFACC by direction of the JFC.
- ✪ Provide EW support to coordinate:
  - ✪ Strategic attack.
  - ✪ Counterair
  - ✪ Counterland
  - ✪ Countersea
  - ✪ Air Mobility Support
  - ✪ Information Operations/Information Warfare (IO/IW).
  - ✪ Combat Search and Rescue.
  - ✪ SOF operations with the Joint Special Operations Task Force/Joint Special Operations Air Component Commander.
- ✪ Perform combat assessment of joint EW operations at the operational and tactical levels.
- ✪ Provide integrated electronic warfare support (ES) for the JFC.

- ✪ Identify JFACC requirements.
- ✪ Integrate and synchronize use of aerospace assets.
- ✪ Task theater ES assets to satisfy JFC requirements.

**If working with allies in a coalition, the EW team will support the Combined Force Air Component Commander (CFACC).**

## EW SUPPORT TO THE COMMANDER, AIR FORCE FORCES (COMAFFOR).

The COMAFFOR provides unity of command, one of the most widely recognized principles of war. The COMAFFOR normally exercises OPCON over all assigned and attached US Air Force forces. EW planners will assist the COMAFFOR in fulfilling the following ADCON responsibilities:

- ✪ Make recommendations to the JFC (or the JFACC, if the COMAFFOR is not the JFACC) on the proper employment of the EW forces of the Air Force component.
- ✪ Accomplish assigned EW tasks.
- ✪ Nominate specific EW units of the Air Force for assignment to theater forces.
- ✪ Organize, train, equip, and sustain subordinate Air Force EW forces for assigned missions.
- ✪ Develop and disseminate force EW protection.
- ✪ Maintain reachback to AFFOR rear and supporting Air Force EW units.
- ✪ Support operational and exercise EW plans as requested.

- ✪ Develop EW program and budget requests that comply with combatant commander guidance on warfighting requirements and priorities.
- ✪ Inform the combatant commander (and any intermediate JFCs) of EW program and budget decisions that may affect joint operation planning.
- ✪ Provide lateral EW interface with Army, Navy, Marines, SOF, and coalition partners.

When the COMAFFOR is delegated OPCON of the Air Force component forces, and there is no JFACC, EW planners will assist the COMAFFOR in fulfilling the following **OPCON responsibilities:**

- ✪ Prepare an EW Estimate of the Situation to support the JFC's Estimate.
- ✪ Develop and recommend EW courses of action to the JFC.
- ✪ Develop an EW strategy and operations plan that state how the COMAFFOR plans to exploit EW capabilities to support the JFC's objectives.
- ✪ Make EW apportionment recommendations to the JFC.
- ✪ Task, plan, coordinate, and allocate the daily EW effort.
- ✪ Function as the integrator for EW for counterair operations, strategic attack, the overall air interdiction effort, and theater airborne reconnaissance and surveillance.
- ✪ Function as the EW interface, as directed by the JFC, for operations such as close air support, air interdiction within the land and naval component AOs, and maritime support.
- ✪ Coordinate EW support for Combat Search and Rescue.

- ✪ Conduct joint EW training, including the training, as directed, of components of other Services in joint operations for which the COMAFFOR has or may be assigned primary responsibility, or for which the Air Force component's facilities and capabilities are suitable.

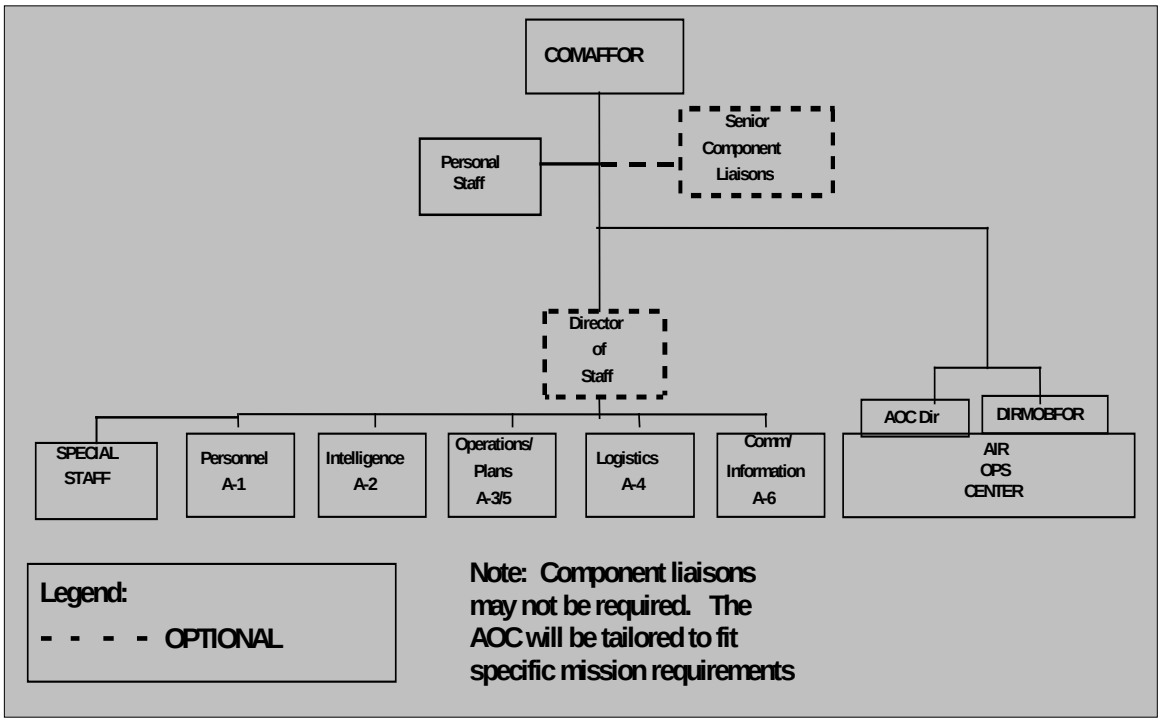
**EFFECTIVENESS OF EW (WORLD WAR II)**

On 7 February 1945 the Fifteenth Air Force lost 25 of the 689 aircraft sent against Vienna (19 to flak). The Fifteenth Air Force hit the city again the next day, but this time it lost none of its 470 bombers. The losses on the first raid were due to the clear weather that helped the gunners and to the Americans' lack of airborne coordination and electronic countermeasures (ECM). The success on the following day was attributed to poorer weather (7/10 to 10/10 overcast) and better American coordination and ECM.

**Kenneth P. Werrell**
**Archie, Flak, AAA, and SAM: A Short Operational History of Ground-Based Air Defense**

## COMAFFOR HEADQUARTERS ORGANIZATION: THE "A-STAFF"

The COMAFFOR headquarters should usually be comprised of normal staff directorates, A-1 through A-6, as well as a special staff. In Deliberate Planning or Crisis Action Planning, the NAF designated as the COMAFFOR will integrate EW experts into the organization.




COMAFFOR Headquarters Organization

The core of the EW function is located in the A-3 as part of the IW functions, although it is critical that the whole IW operation is integrated with the A-2/5/6. The EW personnel will provide these functions:

**Intelligence (A-2)**

- ✪ Coordinate Essential Elements of Information for A-3.
- ✪ Provide the intelligence staff, EW objectives, intent, and plans.
- ✪ Coordinate EW intelligence support from JFC fusion centers, MAJCOM intelligence staffs, theater intelligence agencies, national intelligence agencies, and coalition intelligence sources.

- ✪ Apprise the Director of Intelligence of EW capabilities and limitations of all components and the potential effects on operations.
- ✪ Assist A-2 with EW intelligence support requirements of subordinate units.

## Operations/Plans (A-3/A-5)

- ✪ Organize the operational EW aspects of the headquarters staff.
- ✪ Coordinate operational EW issues with the JFC and component staffs. Typical issues would include
  - ✪ Rules of engagement for EW aerospace forces.
  - ✪ Assist in unit beddown requirements for EW forces.
  - ✪ ATO and ACO EW development requirements.
  - ✪ Provide recommendations for requirements for additional EW forces/capabilities.
  - ✪ Force protection requirements.
- ✪ Identify Essential Elements of Information to A-2.
- ✪ Develop and coordinate the EW Plan and integrate it into the Information Operations Plan that accomplishes the JFC's objectives.
- ✪ Identify service specific EW training requirements and coordinate joint training with other components.
- ✪ Advise COMAFFOR on concepts of EW employment, force planning, and management of EW resources for which he has OPCON/TACON or has established supported/supporting relationships.

- ✪ Provide information on the number and location of all EW air assets.

## Communications and Information (A-6)

- ✪ Coordinate for the A-3 to ensure that frequency allocations and assignments meet technical parameters under host nation agreements, and JTF J-6, deconflict frequencies, coordinate JFRL, and provide communications-electronics operating instructions for assigned forces.
- ✪ Plan, coordinate, and monitor EW related COMSEC procedures and assets.

# Chapter 4

# PLANNING AND EMPLOYMENT

*To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds.*

Mao Tse Tung

## PLANNING

**General.** Electronic warfare planning requires a broad understanding of enemy and friendly capabilities, tactics, and objectives. Employment of EW assets must be closely integrated into, and supportive of, the commander's overall planning effort. This planning requires a multi-disciplined approach with expertise from operations (ground and airborne), intelligence, logistics, communications, and computer services.

**Planning Requirements.** Initial EW plans should be formed prior to hostilities. As the battle progresses, adjustments will be necessary based on current intelligence. Proper EW planning can minimize friendly losses and optimize operational effectiveness. Preconflict plans are long-range in scope. Preparation is not under the pressure of reaction to enemy initiatives. An assessment of enemy versus friendly capabilities is fundamental for preconflict planning. Preconflict plans integrate a strategy for C2 and air defense targeting as well as plans to support primary mission resources. Support to primary mission aircraft depends on assessing critical times and places for friendly aircraft. This support should consider destructive and disruptive systems capabilities. The C2 and air defense prioritized target list must be integrated into an

overall prioritized target list. How and when these targets are attacked depends on the apportionment and allocation process, and the JFC's desired objective. Plans for EW are optimized against enemy system vulnerabilities. Factors influencing EW planning include: available assets; desired effects (exploitation, deception, disruption, or destruction); placement limitations (altitude, range, time, or loads); frequency deconfliction; anticipated EW missions from other services; and authentication requirements.

**Planning Priorities.** As with any operation, the JFC's objective, enemy situation, and assets available impact on the particular priority for employment of limited EW assets. Electronic warfare is task, scenario, and time dependent. The commander's EW plans must be flexible to keep pace with the dynamic combat environment.

**DESERT STORM: First Night**

*Early in the morning of 17 January, 1991, three US Air Force MH-53J Pave Low helicopters led nine US Army AH-64 Apache helicopters across the Saudi Arabia-Iraq border to attack two Iraqi early warning radar sites. Taking down these two sites opened the door for attacks across Iraq by F-117s, other Coalition aircraft and Tomahawk missiles.*

*"After the F-117s and cruise missiles came conventional aircraft. From 0355L to 0420L (H+55 to H+1:20) large numbers of USAF, USN, USMC, RSAF, and RAF aircraft smashed Iraqi air defenses and fields from H-3, an airfield located in western Iraq, to Ahmed Al Jaber, an airfield in occupied Kuwait.. Two packages of aircraft, one a USN package from the Red Sea carriers and the other a USAF package from the south pointed directly at Baghdad. These "gorilla" packages were intended to seem threatening enough to force the Iraqis to hurl their air resources in defense. Air Force ground-launched BQM-34 and navy air-launched TALD pilotless decoys mimicked the radar return of conventional aircraft to further arouse Iraqi radar operators, many already confused by the absence of central control from Kari. They responded by turning on their equipment. Finally, radar-jamming aircraft radiated blanketing electronic emissions that drove the Iraqi radar operators to go to full power in an attempt to break through the interference. Then, the two incoming Coalition flights revealed their true nature and pounced in a shrewd and devastating ruse.*

*Instead of bomb-carrying fighter-bombers, they were radar-killing electronic warriors carrying AGM-88 high-speed anti-radiation missiles (HARMS) designed to home in on SAM and AAA radar. USAF F-4G Wild Weasels alone expended dozens of HARMS in twenty minutes, while USN/USMC F/A-18s fired one-hundred for the night. HARMS filled the air over Baghdad, the site of over one-half of Iraq's SAM and AAA batteries. Foolishly, the Iraqis did not turn off their radars, even when the HARMS fireballed in their midst; as one USAF flight leader averred, "the emitters came on and stayed on for the entire flight of the missiles." This deadly surprise not only destroyed many Iraqi radars, it also terrified their operators. For the rest of the war, they showed great reluctance to use radar and often chose to launch their SAMs with optical or even no guidance. The initial HARM attack and the F-117 bombings of the Kari system left Iraq's integrated air defense system shattered, opening up the country so completely that, within days, Coalition air-to-air tankers regularly operated in Iraqi airspace. Other non-stealthy aircraft pummeled Iraqi airfields.*

***Richard G. Davis, Decisive Force: Strategic Bombing in the Gulf War***

**Force Mix Considerations.** A balance is necessary between dedicated and self-protection EW systems as well as between destructive and disruptive measures. The commander's objectives, the enemy's capabilities, and the equipment available determine the actual force mix. Considerations include the threat, tactics, attrition rates, regeneration factors, friendly and enemy sortie rates, technological risks, and warning times. The goal of dedicated electronic assets is to support the objectives of the joint force commander and the air component commander. The targets for dedicated electronic assets include C2 subsystems, offensive and defensive full-spectrum electronic systems and air defense associated electronic subsystems. The effectiveness of offensive electronic assets can be measured by the degradation of the adversary

C2 . Defensively, effectiveness can be measured by retention of friendly forces C2 and survivability. The effectiveness of destructive assets can be measured by analyzing the effect on the enemy. The desired impact will be specified in the overall objectives provided by the JFC.

Electronic warfare jammers vary in effective range, power and modulation. Electro-magnetic radiations can be aimed and focused, but do not stop at definitive geographic boundaries or discrete altitudes. Theater electromagnetic spectrum (frequency) interface deconfliction procedures are necessary to minimize mutual interference and degradation of friendly efforts. Frequency management is enhanced if jammer system design includes directional antennas, capabilities exist to lock-out frequencies, realistic restricted frequencies are stated by friendly forces, and a command and control process exists which is responsive to real-time frequency changes.

The EW mix is a function of the detection, denial, deception, disruption, and destruction effort necessary to support desired objectives. Considerations include the threat, tactics, attrition rates, regeneration factors, friendly and enemy sortie rates, technological risks, and warning times.

**Intelligence Support.** An accurate and available intelligence base is the foundation for effective EW planning and employment. Intelligence supports EW through three functions. First, constant analysis by various scientific and technical centers guards against hostile technical surprise. Second, indications and warnings (I&W) centers provide tactical and strategic warning to our forces. Third, intelligence continually monitors threat systems to support reprogramming of all systems.

Specifically, intelligence supports EW by providing a technical threat description and a tailored threat environment description. Electronic warfare planning requires parametric and employment data to prioritize targets and defense tasks. All-source intelligence assets are required to support both offensive and defensive EW planning. To be of value, these assets must provide timely intelligence and be responsive to the commander's needs. Intelligence support includes establishing and maintaining comprehensive support databases. The size and detail of a given database depend on EW user requirements. Intelligence data must be filtered, integrated, and evaluated so the EW planners and decision-makers are not overloaded with excessive or meaningless data.

**Logistics Support.** Readiness and sustainability of electronic assets are directly related to the quality of logistics planning. EW logistics programs should be developed in balance with modernization efforts and the operating capability each category of resources provides. Emphasis must be on total effectiveness to maximize EW capabilities.

## EMPLOYMENT

> *"The immense number of coalition aircraft requesting Wild Weasel and EF-111A support far outstripped their capability to support all missions."*
>
> USCENTAF Electronic Combat in Desert Shield and
> Desert Storm After Action Report, October 1991

**General.** The employment of EW capabilities to affect an adversary can yield a tremendous advantage to US military forces. EW objectives must be clearly established, support overall national and military objectives, and include identifiable indicators of success.

**Combatant Commanders.** Combatant commanders must carefully consider the potential of EW. Combatant commanders should:

- ✪ Integrate EW capabilities into deliberate and crisis action planning in accordance with appropriate policy and doctrine.
- ✪ Ensure maximum coordination among EW and other information operations intelligence and communications support activities for maximum effect and to reduce electronic fratricide.
- ✪ Incorporate EW tactics, techniques, and procedures into exercises and training events using the Joint Training Process.
- ✪ Identify EW capability requirements and submit appropriate mission needs statements.
- ✪ Develop EW intelligence requirements In support of all pertinent operation plans.
- ✪ Identify EW education and training requirements.

**Employment Roles.** EW may be conducted in a variety of situations and circumstances across the range of military operations and may have their greatest impact in the initial steps of a crisis. EW should be employed to attack the enemy according to established principles of warfare. The decision to employ EW should be based not only on overall joint campaign or operation objectives, but also on the risks of possible adversary responses and other potential effects on the campaign or operation.

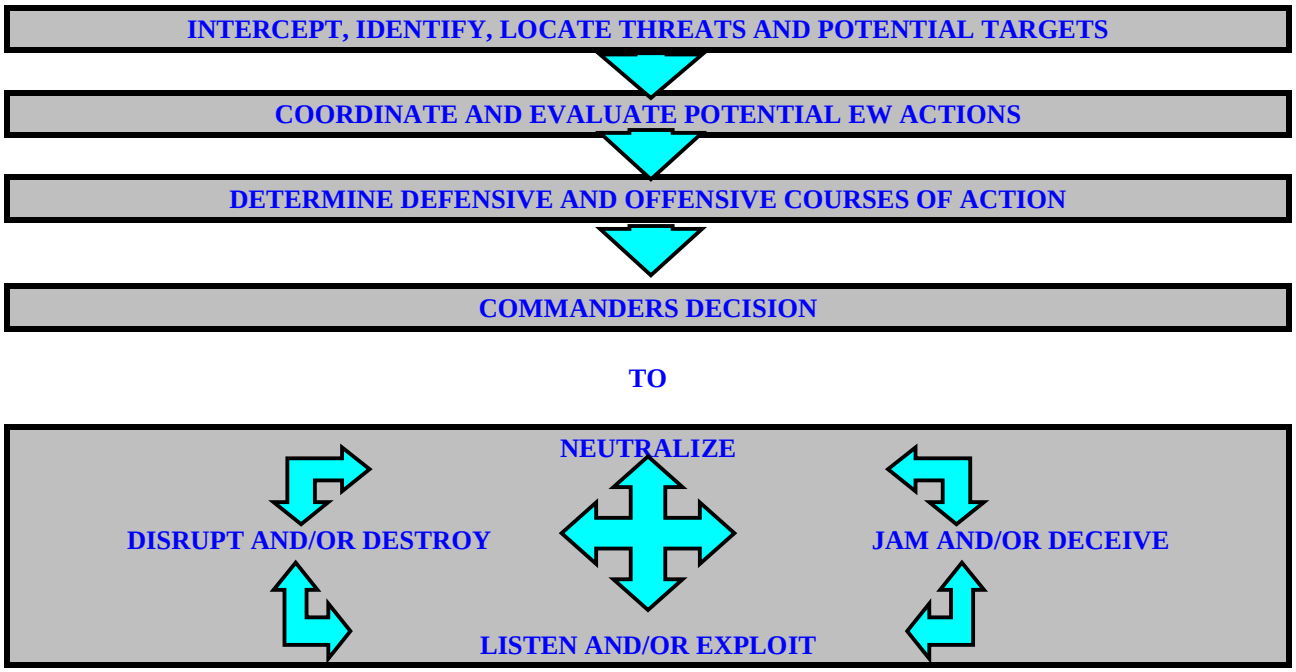



**Figure 4-1, EW EMPLOYMENT PROCESS**

**EW Applications Across the Spectrum of Conflict**. Based on an understanding of the tenets of EW discussed in chapter 2, the employment of EW in the theater must consider several factors. There are several EW applications that amount to an escalation in the utilization of the electromagnetic spectrum. For example, low orders of EW activity such as collection or exploitation have different consequences to the operation than lethal SEAD destroy options. The Air Force will conduct operations across the different levels of war and these operations are affected by the electromagnetic spectrum. This includes wide range of missions that goes from peacetime operations to war. The application of EW in Military Operations Other Than War (MOOTW) will probably be different. It is a theater commander's responsibility to determine the level of EW application to operations under his control. Although it is relatively easy to determine the level of EW application during war due to the fact that all EW measures (lethal and non-lethal) are permitted, most Air Force operations fall short of conflict.

**Military Operations Other than War (MOOTW).** These missions are frequently characterized by operations into nations openly friendly to the US; however, some nation-states are unstable and may include elements that are actively hostile toward the United States. Man Portable Air Defense Systems (MANPAD) and other infrared/electro optical systems are known to be in the hands of terrorist and criminal groups. During peaceful missions to friendly nations, armed opposition factions can make the use electronic attack measures such as the employment of flares an operational requirement. Several EW applications are available MOOTW. EW assets are available for tasking at the discretion of the commander for a variety of missions. Nearly all non-lethal options are available, but it is the commander's responsibility to define these options in the Rules of Engagement/Operations Order (OPORD) or other governing directive. Although electronic attack options such as jamming are generally considered hostile, they may be necessary to protect the tasked forces.

**Crisis/Contingency/War.** Overwhelming density and potential lethality of the tactical air defense system impacts mission effectiveness and the survivability of Air Force missions. Increased sortie survivability is the major consideration for air operations in an EW environment. In combat, it is unlikely that air operations will be unable to avoid enemy defenses because they defend the desired targets. Survivability enhancements from properly composed force packages are necessary actions of JTF commanders.

**BEKAA VALLEY (1982)**

"On 9 June the IAF took on the Syrian air defenses in the Bekaa Valley with a complex yet carefully planned, coordinated, and executed attack. The Israelis used air- and ground-launched drones as decoys to activate Syrian radar. This allowed the Israeli EC-135s to obtain the location and frequency of the Syrian radars and in turn to rapidly relay this information to strike elements. The Israelis thereby coupled real-time intelligence with rapid response to give their pilots precise locations of the SAMs and accurate tuning information for their jamming equipment. In the electronics war, the IAF used ECM pods, chaff rockets, possibly chaff from drones, and standoff jammers in CH-53, Boeing 707, and Arava transports. The Israeli airmen employed diversionary tactics, precise timing, sharply executed low-level tactics, and weapons such as ARMs, standoff weapons, iron bombs, and cluster munitions. In addition, the Israelis used a new surface-to-surface ARM, the Wolf missile. Ground forces fired artillery, launched ground assaults along the front, and just before the air attack took out a control center with a commando raid. The Syrians did not help their own cause, as they failed to dig in, poorly sited their radar, and ignited smoke screens that guided rather than confused the IAF. On the first day, the IAF destroyed 17 missile batteries and severely damaged two others. The Syrians pushed more SAM units into the Bakaa Valley, but to no avail. On the second day of the action, the IAF destroyed 11 more missile batteries. On 24 July the Israelis knocked out three batteries of SA-8s. A few days later, they destroyed some SA-9s. Reportedly, the IAF destroyed four SA-9 batteries in September."

**Kenneth P. Werrell**
**Archie, Flak, AAA, and SAM: A Short Operational History of Ground-Based Air Defense**

# Chapter 5

# EQUIP AND SUSTAIN

> *The unresting progress of mankind causes continual change in the weapons; and with that must come a continual change in the manner of fighting,…."*
>
> A. T. Mahan

## GENERAL.

Air Force MAJCOMS are responsible to train and equip forces for employment by warfighting CINCs. In the process of equipping forces for information operations/electronic warfare, MAJCOMS must plan for, acquire, and field the parts, supplies, munitions, support equipment, support personnel, and communications infrastructure to sustain the EW capabilities of forces deployed or in garrison. The following major areas are of particular concern to EW programs.

**System Engineering.** The system design should be driven by user requirements, the current and projected threats, and concept of operations. To achieve this versatility, the system design must be generic, robust, and easily expandable or modifiable to meet the threat. To the maximum extent possible, EW systems should be an integral part of the weapon system design. EW systems should be designed to accept changes that counter new and evolving threats. These design features ensure EW equipment is not only reactive to threat changes but that it anticipates what the threat is likely to do in response to our capabilities, and planning to counter those responses. EW systems must be able to operate in a dense environment of both friendly and

**Radar Countermeasures**

When bombing raids over Germany were started, the extent of the German radar development was immediately realized. Not only were enemy interceptor aircraft equipped with airborne radar capable of locating our bombers through the heaviest overcast, or at night at distances up to 10 miles, but our aircraft were also being damaged by antiaircraft fire directed by a very effective gun-laying radar known as the "Small Wurzburg." A similar radar, the "Giant Wurzburg," was used by the Germans for fighter control, while a 125-MHz set, the "Freya," was used for early warning. In the initial days of our bombing against Germany, losses were extremely high due to the enemy's electronic weapons. The Giant Wurzburg was one of the first modern radars, since it combined a fire-control capability with its search function. Its antenna was a 25-foot diameter parabolic reflector which operated at a frequency of 570 MHz. Several approaches were used to counter these and later German radars.

"Window" (or chaff) was introduced in a raid on Hamburg on the night of July 24-25, 1943. Seven hundred and ninety-one bombers dropped (in addition to bomb loads) one bundle of 2,000 aluminum foil strips every minute-totalling over 2 1/2 million strips weighing 20 tons. To the enemy radar defenses, this represented approximately 12,000 aircraft over Hamburg and had devastating effect on the enemy. The chaff drop reduced losses from 5.4 percent to 1.5 percent and was spectacular justification for the British Air Force (RAF) RCM. After 2 months of use by the British, the RAF estimated that chaff had been responsible for saving at least 200 planes and between 1,200 and 1,500 men.

**AFP 51-45**
**15 September 1987**

hostile systems. A means of maintaining security for possible war reserve modes must be incorporated in the system design to avoid compromise of our system capability. EW systems are subject to unintended interactions or mutual interference with other systems on the same platform, other aircraft in a formation, and other systems operating throughout the theater. Compatibility, interoperability, and frequency deconfliction of EW systems must be integrated across the electronic battlespace.

**Electronic Counter-Counter Measures (ECCM).** EW systems evolve continuously as engineers develop improved capabilities and countermeasures to hostile capabilities. All weapons systems (not just EW systems) must have effective ECCM to operate in a hostile EW environment. Systems in development must include ECCM considerations at the beginning of the design cycle and be able to accept ECCM updates (hardward and software) to keep pace with the evolving EW threat. Continuous intelligence support is required to look for evolutionary and revolutionary developments adversary threat systems so that the appropriate ECCM can be designed and deployed.

**Communications:** Communication plans are directly related to electronic warfare plans. Communications plans provide for redundancy, work-arounds, and regeneration of required friendly communications systems. The communication staff or representative is required when EW frequency deconfliction and defensive information operations plans are worked. Communications support is critical for effective intelligence support and reprogramming actions for EW systems.

**Reprogramming and Electronic Data Base Support**. EW operations demand large amounts of data on US and friendly systems and operations in addition to intelligence support on hostile forces. Programming and reprogramming of EW systems and much of the targeting work is based on parametric databases, electronic orders of battle (EOB), and communications network databases. **An accurate EOB, and a communications network database, must be maintained to ensure effective EW sustainment, planning, and execution.** These databases are developed from US and friendly data exchanges and all-source intelligence collection and reporting. An EW system's flexibility depends on its capability to adapt to changing threats. EW systems depend on rapid reprogramming, which is enabled by rapid communication of intelligence data to operators and reprogramming centers, where updated mission software is created and transmitted to the field. This Electronic Warfare Integrated Reprogramming (EWIR) process depends on MAJCOM, System Program Office (SPO), Air Logistics Center (ALC), and reprogramming center support. JFACCs /COMAFFOR should ensure the reprogramming process is accomplished for their forces.

**Intelligence Support. An accurate and available intelligence base is the foundation for effective EW planning and employment**. Intelligence supports EW by using various scientific and technical centers to guard against hostile technical surprise. Indications and warnings (I&W) centers provide tactical and strategic warning for friendly forces. Finally, intelligence monitors threat systems to support reprogramming.

# CHAPTER 6

# EDUCATION AND TRAINING

> ***In the profession of war the rules of the art are never violated without drawing punishment from the enemy who is delighted to find us at fault. An officer can spare himself many mistakes by improving himself.***
>
> Frederick the Great

The effective employment of EW in support of operational objectives depends on commanders, aircrews, and planners understanding EW system capabilities to be well versed in the integration of EW at all levels of operations. Specialized education and realistic training in IW execution and EW employment achieve this objective. Specialized schools or classes are a valuable tool that can provide units commanders and instructors with in-depth IW and EW skills.

## EDUCATION

**Basic. High levels of proficiency are required for everyone involved with electronic warfare employment.** All aircrew must receive basic EW education through programs initiated at their unit. Other specialties must be familiar with EW to design and acquire systems, provide intelligence support, reprogram mission data and perform other critical support tasks.

**Advanced.** Specialized and comprehensive training is required to provide the unique skills that are essential for individuals assigned to the air operations staff. **These individuals are the key elements in effective integration of EW at all levels of the air campaign.** They will be

expected to have an in-depth knowledge of national assets, an understanding of targeting, and to provide the commander with an EW package tailored to the operational objectives.

**Senior. Senior officers must be familiar and well versed with the basic tenets of EW employment and integration.** Not only are they tasked as commanders for air operations during times of conflict, they are also involved with critical decisions on equipping, sustaining, and employing our forces to meet national objectives.

**TRAINING**:

**Training must have attainable objectives that are specific, relevant, and necessary for combat.** Employment of EW during training should be accomplished in a realistic combat environment and should include operations with actual combat equipment in realistic scenarios. Employment constraints must be followed; however, methods may be devised to minimize the impact of these restrictions on training. A review of deficiencies noted from past operations and exercises provides a valuable training resource. Emphasis should be placed on evaluating EW tactics, procedures, and safety constraints to optimize EW employment.

Electronic warfare training must be emphasized on a continuing basis (daily, weekly, quarterly, etc.) and must include all personnel who may encounter direct or indirect, friendly or hostile EW situations. **EW impacts personnel in many areas to include: flight operations; air weapons; communications; intelligence; maintenance; security; and other support functions.** Specialized exercises (Blue Flag, Green Flag, etc.) provide hands-on experience at the tactical, operational and strategic level.

Unit training should include enemy threat system characteristics, capabilities, and limitations. **Operators must train against an integrated air defense system that includes all types of threats: surface-to-air, air-to-air, and electronic warfare systems.** Proficiency must be maintained in the operation of EW equipment as well as the employment of EW tactics. Training should be realistic, based on accurate threat capabilities, and must provide accurate and rapid feedback to the trainees. The motto of EW training remains: **Train with EW, Fight with EW.**

***At the Heart of Warfare lies doctrine . . .***

# SUGGESTED READING

CJCSI 3210.01, Joint Information Warfare Policy

De Arcangelis, Mario. Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanon Conflicts. Poole, Dorset: Blandford Press, 1985.

DOD Directive S-3600.1, Information Operations

Joint Pub 3-13, Joint Doctrine for Information Operations (Draft)

Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare

Joint Pub 3-51, Joint Doctrine for Electronic Warfare

Joint Pub 3-58, Joint Doctrine for Military Deception

Global Engagement: A Vision for the 21st Century Air Force.

Munro, Neil. The Quick and the Dead: Electronic Cobat and Modern Warfare. New York: St Martins's Press, 1991.

Price, Alfred. The History of US Electronic Warfare, Volume I. The Association of Old Crowes, 1984.

Price, Alfred. The History of US Electronic Warfare, Volume II. The Association of Old Crowes, 1989.

Werrell, Kenneth P. Archie, Flak, AAA, and SAM. Maxwell AFB, AL: Air University Press, 1988.

# GLOSSARY

## *ABBREVIATIONS AND ACRONYMS*

| | |
|---|---|
| AAA | antiaircraft artillery |
| ACQ | acquisition |
| AFCERT | Air Force Computer Emergency Response Team |
| AFDD | Air Force Doctrine Document |
| AFIWC | Air Force Information Warfare Center |
| AFNCC | Air Force Network Control Center |
| AFOSI | Air Force Office of Special Investigation |
| AFSOF | Air Force special operations forces |
| AFSPC | Air Force Space Command |
| AFSST | Air Force Space Support Team |
| AI | air intercept |
| AIA | Air Intelligence Agency |
| AOC | air operations center |
| AOR | area of responsibility |
| ARM | antiradiation missile measures |
| ATO | air tasking order |
| AWACS | Airborne Warning and Control System |

| | |
|---|---|
| BCD | battlefield coordination detachment |
| $C^2$ | command and control |
| $C^4I$ | command, control, communications, computer systems, and intelligence |
| CERT | computer emergency response team |
| CI | counterinformation |
| CIA | Central Intelligence Agency |
| CIJ | close in jamming |
| CINC | commander in chief |
| CJCSI | Chairman, Joint Chiefs of Staff Instruction |
| COA | course of action |
| COMAFFOR | commander, air force forces |
| COMAFSPACE | Commander, Air Force Space Command |
| COMINT | communications intelligence |
| COMPUSEC | computer security |
| COMSEC | communications security |
| DCI | defensive counterinformation |
| DII | defense information infrastructure |
| DISA | Defense Information Systems Agency |
| DOD | Department of Defense |
| DODD | Department of Defense Directive |

| | |
|---|---|
| DT&E | developmental test and evaluation |
| | |
| EA | electronic attack |
| ECAC | electromagnetic compatibility analysis center |
| ECC | electronic warfare coordinator |
| ECM | electronic countermeasures |
| ECCM | electronic counter-countermeasures |
| EEFI | essential elements of friendly information |
| EEI | essential elements of information |
| ELINT | electronic intelligence |
| ELSEC | electronic security |
| EMCON | emission control |
| EMI | electromagnetic interference |
| EMP | electromagnetic pulse |
| E-O | electro-optics |
| EOB | electronic order of battle |
| ESM | electronic warfare support |
| EM | electromagnetic |
| EMC | electromagnetic compatibility |
| EP | electronic protection |
| ES | electronic warfare support |
| EW | electronic warfare |
| EWEP | electronic warfare evaluation program |

| | |
|---|---|
| EWIR | electronic warfare integrated reprogramming |
| EWO | electronic warfare officer |
| | |
| FMC | frequency management center (compatibility) |
| | |
| GCI | ground-controlled intercept |
| GII | global information infrastructure |
| GPS | global positioning system |
| | |
| HARM | high-speed antiradiation missile |
| | |
| IA | information assurance |
| IADS | integrated air defense system |
| ICS | internal countermeasures set |
| IED | imitative electronic deception |
| IFF | identification, friend, or foe |
| IFFN | identification, friend, foe, or neutral |
| INEWS | integrated electronic warfare system |
| I & W | indications and warning |
| INFOSEC | information security |
| IO | information operations |
| IP | information protection (also called info protect) |
| IW | information warfare |

| | |
|---|---|
| IWS | information warfare squadron |
| | |
| JAG | Judge Advocate General |
| JAOC | joint air operations center |
| JASOP | joint air and space operations plan |
| JC2WC | Joint Command and Control Warfare Center |
| J-C3CM | joint command, control, and communications counter |
| JIWC | Joint Information Warfare Center (Kelly AFB) |
| JFACC | joint force air component commander |
| JFC | joint force commander |
| JIPTL | joint integrated prioritized target list |
| JOA | joint operations area |
| J-SEAD | joint suppression of enemy air defenses |
| JSTARS | joint surveillance, target attack radar system |
| JTF | joint task force |
| | |
| LAN | local area network |
| LEA | Law Enforcement Agencies |
| LNO | liaison officer |
| | |
| MAAP | master air attack plan |
| MAJCOM | major command |

| | |
|---|---|
| MED | manipulative electronic deception |
| MIJI | meaconing, intrusion, jamming, and interference |
| MOOTW | military operations other than war |
| | |
| NCA | National Command Authorities |
| NII | national information infrastructure |
| NRT | near real time |
| NSA | National Security Agency |
| | |
| | |
| OCI | offensive counterinformation |
| OPCON | operational control |
| OPLAN | operation plan |
| OPORD | operation order |
| OPSEC | operations security |
| OT&E | operational test and evaluation |
| | |
| PGM | precision-guided munitions |
| PNP | precision navigation and positioning |
| PSYOP | psychological operations |
| | |
| ROE | rules of engagement |
| R&D | research and development |

| | |
|---|---|
| REC | radio electronic combat |
| RECCE | reconnaissance |
| RWR | radar warning receiver |
| | |
| SAM | surface to air missile |
| SEAD | suppression of enemy air defenses |
| SED | simulative electronic deception |
| SIGINT | signals intelligence |
| SIOP | Single Integrated Operational Plan |
| SOC | space operations center |
| SOF | special operations forces |
| SOJ | stand off jamming |
| SSM | surface-to-surface missile |
| SPINS | special instructions |
| STO | special technical operations |
| | |
| T&E | test and evaluation |
| TACC | tactical air control center |
| TACS | tactical air control system |
| TDO | tactical deception officer |
| TEL | transporter, erector, launcher |
| TELINT | telemetry intelligence |
| TFECIC | Tactical Fighter Electronic Combat Instructors Course |

| | |
|---|---|
| TMAP | Telecommunications Monitoring and Assessment Program |
| TSCM | technical surveillance countermeasures |
| TPFDD | time-phased force and deployment data |
| TW/AA | tactical warning and attack assessment |
| | |
| USCINCSPACE | Commander-in-Chief, United States Space Command |
| | |
| VMC | visual meteorological conditions |
| | |
| WARM | wartime reserve mode |

## ***Definitions***

*acoustic jamming* - (DOD) The deliberate radiation or reradiation of mechanical or electroacoustic signals with the objectives of obliterating or obscuring signals which the enemy is attempting to receive and of deterring enemy weapon systems. See also barrage jamming; electronic warfare; jamming; spot jamming. (JP 1-02)

*active air defense*-(DOD, NATO) Direct defensive action taken to nullify or reduce the effectiveness of hostile air action. It includes such measures as the use of aircraft, air defense weapons, weapons not used primarily in an air defense role, and electronic warfare. See also air

defense. (JP 1-02)

*antiradiation missile* - (DOD, NATO) A missile which homes passively on a radiation source. See also guided missile. (JP 1-02)

***air operations center*** - (DOD) The principal air operations installation from which aircraft and air warning functions of combat air operations are directed, controlled, and executed. It is the senior agency of the Air Force Component Commander from which command and control of air operations are coordinated with other components and Services. Also called AOC. (JP 1-02)

***air tasking order*** - (DOD) A method used to task and disseminate to components, subordinate units, and command and control agencies projected sorties/capabilities/forces to targets and specific missions. Normally provides specific instructions to include call signs, targets, controlling agencies, etc., as well as general instructions. Also called ATO. (JP 1-02)

***barrage jamming*** - (DOD) Simultaneous electromagnetic jamming over a broad band of frequencies. See also jamming. (JP 1-02)

*camouflage* - (DOD, NATO) The use of natural or artificial material on personnel, objects, or tactical positions with the aim of confusing, misleading, or evading the enemy. See also countersurveillance. (JP 1-02)

*chaff* - (DOD) Radar confusion reflectors, which consist of thin, narrow metallic strips of various lengths and frequency responses, used to reflect echoes for confusion purposes. See also rope; rope-chaff; window. (JP 1-02)

*command, control, communications, and computer systems* - (DOD) Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations. Also called C4 systems. See also command and control; tactical command, control, communications, and computer system(s). (JP 1-02)

*command and control* - (DOD) The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1-02)

*command and control system* - (DOD) The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (JP 1-02)

*command and control warfare* - (DOD) The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually

supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information warfare in military operations and is a subset of information warfare. Command and control warfare applies across the range of military operations and all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. See also command and control; electronic warfare; intelligence; military deception; operations security; psychological operations. (JP 1-02)

*communication deception* - (DOD) Use of devices, operations, and techniques with the intent of confusing or misleading the user of a communications link or a navigation system. (JP 1-02)

*communications intelligence* - (DOD) Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT. (JP 1-02)

*communications security* - (DOD) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes: cryptosecurity, transmission security, emission security, and physical security of

communications security materials and information. a. cryptosecurity--The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. transmission security--The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. emission security--The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. physical security--The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JP 1-02)

*computer security* - (DOD) The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. Also called COMPUSEC. See also communications security. (JP 1-02)

*concept of operations* - (DOD) A verbal or graphic statement, in broad outline, of a commander's assumptions or intent in regard to an operation or series of operations. The concept of operations frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operations to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. Also called commander's concept. (JP 1-02)

*control* - (DOD) 1. Authority which may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. 2. In mapping, charting,and photogrammetry, a collective term for a system of marks or objects on the Earth or on a map or a photograph, whose positions or elevations, or both, have been or will be determined. 3. Physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. 4. An indicator governing the distribution and use of documents, information, or material. Such indicators are the subject of intelligence community agreement and are specifically defined in appropriate regulations. See also administrative control; operational control; tactical control. (JP 1-02)

*counterdeception* - (DOD) Efforts to negate, neutralize, diminish the effects of, or gain advantage from, a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. See also deception. (JP 1-02)

*countermeasures* - (DOD) That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. See also electronic warfare. (JP 1-02)

*deception* - (DOD, NATO) Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. See also counterdeception; military deception. (JP 1-02)

*directed energy* - (DOD) An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. Also called DE. See also directed-energy device; directed-energy weapon. (JP 1-02)

*directed-energy warfare* - (DOD) Military action involving the use of directed-energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Also called DEW. See also directed energy; directed-energy device; directed-energy weapon; electromagnetic spectrum; electronic warfare. (JP 1-02)

***defensive counterinformation***-Those actions that protect our information, information systems, and information operations from any potential adversary. Also called **DCI**.

*electromagnetic compatibility* - (DOD) The ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness. Also called EMC. See also electromagnetic spectrum; electronic warfare; spectrum

management. (JP 1-02)

*electromagnetic deception* - (DOD) The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are: a. manipulative electromagnetic deception--Actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces. b. simulative electromagnetic deception--Actions to simulate friendly, notional, or actual capabilities to mislead hostile forces. c. imitative electromagnetic deception--The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. See also electronic warfare. (JP 1-02)

*electromagnetic environmental effects* - (DOD) The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility/electromagnetic interference; electromagnetic vulnerability; electromagnetic pulse; electronic protection, hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and p-static. Also called E3. (JP 1-02)

*electromagnetic interference* - (DOD) Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a

result of spurious emissions and responses, intermodulation products, and the like. Also called EMI. (JP 1-02)

*electromagnetic intrusion* - (DOD) The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. See also electronic warfare. (JP 1-02)

*electromagnetic jamming* - (DOD) The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. See also electromagnetic spectrum; electronic warfare; spectrum management. (JP 1-02)

*electromagnetic pulse* - (DOD) The electromagnetic radiation from a nuclear explosion caused by Compton-recoil electrons and photoelectrons from photons scattered in the materials of the nuclear device or in a surrounding medium. The resulting electric and magnetic fields may couple with electrical/electronic systems to produce damaging current and voltage surges. May also be caused by nonnuclear means. Also called EMP. (JP 1-02)

*electromagnetic radiation* - (DOD) Radiation made up of oscillating electric and magnetic fields and propagated with the speed of light. Includes gamma radiation, X-rays, ultraviolet, visible, and infrared radiation, and radar and radio waves. (JP 1-02)

*electromagnetic spectrum* - (DOD) The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. See also electronic warfare. (JP 1-02)

*electromagnetic vulnerability* - (DOD) The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of electromagnetic environmental effects. Also called EMV. (JP 1-02)

*electronic attack* - See electronic warfare. (JP 1-02)

*electronic intelligence* - (DOD) Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. See also electronic warfare; intelligence; signals intelligence; telemetry intelligence. (JP 1-02)

*electronic masking* - (DOD, NATO) The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures/signals intelligence, without significantly degrading the operation of friendly systems. (JP 1-02)

*electronics security* - (DOD) The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and

study of noncommunications electromagnetic radiations, e.g., radar. (JP 1-02)

*electronic warfare* - (DOD) Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack. That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection. That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence, and electronics intelligence. See also command and control warfare; communications intelligence; directed-

energy device; directed-energy warfare; directed-energy weapon; electromagnetic compatibility; electromagnetic deception; electromagnetic hardening; electromagnetic jamming; electromagnetic spectrum; electronics intelligence; frequency deconfliction; signals intelligence; spectrum management; suppression of enemy air defenses. (JP 1-02)

*electro-optics* - (DOD, NATO) The technology associated with those components, devices and systems which are designed to interact between the electromagnetic (optical) and the electric (electronic) state. (JP 1-02)

*emission control* - (DOD) The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. minimize mutual interference among friendly systems; and/or c. execute a military deception plan. Also called EMCON. See also electronic warfare. (JP 1-02)

*essential elements of friendly information* - (DOD) Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. Also called EEFI. (JP 1-02)

*essential elements of information* - (DOD) The critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. Also called EEI. (JP 1-02)

*information* - (DOD) 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

***information assurance***—Those actions and measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities. Also called **IA**.

***information attack*—**Any activity taken to manipulate or destroy an adversary's information systems without necessarily changing visibly the physical entity within which it resides.

***information operations***-- Those actions taken to gain, exploit, defend or attack information and information systems (AFDD 1, p. 44). Also called **IO**.

***information superiority***--The ability to collect, control, exploit and defend information while denying an adversary the ability to do the same (AFDD 1). One of six Air Force core competencies.

***information systems***--The means used to acquire, transform, store, or transmit information. (This term promulgated in DODD S-3600.1 of 9 Dec 96.)

***information warfare*—**Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called **IW**.

(Joint Pub 3-13, Preliminary Coordination Draft) (This term promulgated in DODD S-3600.1 of 9 Dec 96.) *[Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems.]* {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

*integration* - (DOD) 1. A stage in the intelligence cycle in which a pattern is formed through the selection and combination of evaluated information. 2. In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print, or the process by which several photographic images are combined into a single image. (JP 1-02)

*joint force* - (DOD) A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. See also joint force commander. (JP 1-02)

*joint force air component commander* - (DOD) The joint force air component commander derives authority from the joint force commander who has the authority to exercise operational control, assign missions, direct coordination among subordinate commanders, redirect and organize forces to ensure unity of effort in the accomplishment of the overall mission. The joint force commander will normally designate a joint force air component commander. The joint force air component commander's responsibilities will be assigned by the joint force commander (normally these would include, but not be limited to, planning, coordination, allocation, and tasking based on the joint force commander's apportionment decision). Using the joint force commander's guidance and authority, and in coordination with other Service component

commanders and other assigned or supporting commanders, the joint force air component commander will recommend to the joint force commander apportionment of air sorties to various missions or geographic areas. Also called JFACC. See also joint force commander. (JP 1-02)

*joint force commander* - (DOD) A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. Also called JFC. See also joint force. (JP 1-02)

*joint suppression of enemy air defenses* - (DOD) A broad term that includes all suppression of enemy air defense activities provided by one component of the joint force in support of another. Also called J-SEAD. See also air defense suppression; suppression of enemy air defenses. (JP 1-02)

*joint task force* - (DOD) A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. Also called JTF. (JP 1-02)

*meaconing* - (DOD, NATO) A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. (JP 1-02)

***MIJI***—(AFR 55-3)—Meaconing, intrusion, jamming and interference of electromagnetic systems. Meaconing, intrusion, and jamming are further defined as deliberate actions by unfriendly countries. Events attributed to friendly countries or another United States activity that technically qualify as meaconing, intrusion, or jamming will be evaluated as interference.

*military deception* - (DOD) Actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are: a. strategic military deception--Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations. b. operational military deception--Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations. c. tactical military deception--Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements. d. Service military deception--Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems. e. military deception in support of operations security (OPSEC)--Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent

compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities. See also deception. (JP 1-02)

*National Command Authorities* - (DOD) The President and the Secretary of Defense or their duly deputized alternates or successors. Also called NCA. (JP 1-02)

***offensive counterinformation***--Offensive IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems. Also called **OCI**.

*operations security* - (DOD) A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. See also command and control warfare; operations security indicators; operations security measures; operations security planning guidance; operations security vulnerability. (JP 1-02)

*psychological operations* - (DOD) Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and

ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. See also consolidation psychological operations; overt peacetime psychological operations programs; perception management. (JP 1-02)

*radar* - (DOD) A radio detection device that provides information on range, azimuth and/or elevation of objects. (JP 1-02)

*radar camouflage* - (DOD, NATO) The use of radar absorbent or reflecting materials to change the radar echoing properties of a surface of an object. (JP 1-02)

*radar clutter* - (DOD, NATO) Unwanted signals, echoes, or images on the face of the display tube, which interfere with observation of desired signals. (JP 1-02)

*radar countermeasures* - See electronic warfare; chaff. (JP 1-02)

*radar coverage* - (DOD, NATO) The limits within which objects can be detected by one or more radar stations. (JP 1-02)

*radar deception* - See electromagnetic deception. (JP 1-02)

*signals intelligence* - (DOD) 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. See also communications intelligence; electronics intelligence; intelligence; foreign instrumentation signals intelligence. (JP 1-02)

*spot jamming* - (DOD, NATO) The jamming of a specific channel or frequency. See also barrage jamming; electronic warfare; jamming. (JP 1-02)

*suppression* - (DOD) Temporary or transient degradation by an opposing force of the performance of a weapons system below the level needed to fulfill its mission objectives. (JP 1-02)

*suppression mission* - (DOD) A mission to suppress an actual or suspected weapons system for the purpose of degrading its performance below the level needed to fulfill its mission objectives at a specific time for a specified duration. (JP 1-02)

*suppression of enemy air defenses* - (DOD) That activity which neutralizes, destroys, or temporarily degrades surface-based enemy air defenses by destructive and/or disruptive means. Also called SEAD. See also electromagnetic spectrum; electronic warfare. (JP 1-02)

*tactical air control group* - (DOD) 1. land-based--A flexible administrative and tactical component of a tactical air organization which provides aircraft control and warning functions ashore for offensive and defensive missions within the tactical air zone of responsibility. 2. ship-based--An administrative and tactical component of an amphibious force which provides aircraft control and warning facilities afloat for offensive and defensive missions within the tactical air command area of responsibility. (JP 1-02)

*tactical air control system* - (DOD, NATO) The organization and equipment necessary to plan, direct, and control tactical air operations and to coordinate air operations with other Services. It is composed of control agencies and communications-electronics facilities which provide the means for centralized control and decentralized execution of missions. (JP 1-02)

*tactical deception group* - (DOD) A task organization that conducts deception operations against the enemy, including electronic, communication, visual, and other methods designed to misinform and confuse the enemy. (JP 1-02)

*technical surveillance countermeasures* -(DOD) Includes techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidics, and acoustic means, as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected.

Also called TSCM. See also counterintelligence. (JP 1-02)

*telemetry intelligence*- (DOD) Technical intelligence derived from the intercept, processing, and analysis of foreign telemetry. Telemetry intelligence is a category of foreign instrumentation signals intelligence. Also called TELINT. See also electronics intelligence; intelligence; foreign instrumentation signals intelligence. (JP 1-02)

*wartime reserve modes*- (DOD) Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. Wartime reserve modes are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use. Also called WARM. (JP 1-02)

*wild weasel*-(DOD, NATO) An aircraft specially modified to identify, locate, and physically suppress or destroy ground based enemy air defense systems that employ sensors radiating electromagnetic energy. (JP 1-02)